A Light yet Low-delay Authentication System for the Internet of Vehicles Based on Blockchain

Guokai Zhao*, Tongtong Zhang†, Yankai Xie*, Jin Ma†, Chi Zhang*, and Lingbo Wei‡*
*School of Cyberspace Science and Technology
University of Science and Technology of China, Hefei, Anhui 230027, P. R. China
†School of Electronic Information and Electrical Engineering
Shanghai Jiao Tong University, Shanghai 200240, P. R. China
‡Institute of Dataspace, Hefei Comprehensive National Science Center, Hefei, Anhui, China
E-mails: guokaizhao@mail.ustc.edu.cn, Lucky-T@sjtu.edu.cn, ykxie@mail.ustc.edu.cn,
heltonma@sjtu.edu.cn, {chizhang, lingbowei}@ustc.edu.cn

***Abstract*—To provide resilience against single points of failure on the Internet of Vehicles Authentication Systems, blockchain-based schemes have emerged as one of the most promising solutions. However, existing schemes fail to preserve anonymity while minimizing both vehicle storage overhead and authentication delay. In this paper, we propose a light blockchain-based authentication scheme that meets anonymity and storage requirements without compromising delays. By incorporating a dynamic accumulator and a customized pseudonym identity strategy, vehicles can outsource most of the storage burden to roadside units while preserving the anonymous authentication of vehicles. Moreover, we adopt an offline/online model, enabling vehicles to preprocess the authentication proof and thereby reduce authentication delays. Additionally, we further enhance the efficiency of preprocessing by dividing vehicles into multiple domains. Security analysis and experiments demonstrate that our scheme can maintain vehicle anonymity without compromising vehicle storage while minimizing authentication delays compared to existing blockchain-based schemes.**

***Keywords*—Internet of vehicles; blockchain; dynamic accumulators; identity authentication**

I. INTRODUCTION

Over the last two decades, the Internet of Vehicles (IoV) has emerged as a key component of intelligent transportation systems. Vehicles in the IoV can efficiently exchange essential security messages in various novel applications, including crash avoidance, route adjustment, and emergency alerts [1]. This facilitates safety enhancements and enhances traffic efficiency. However, the security issues that have emerged correspondingly have become the primary challenges of the IoV, as seen with the potential danger posed by falsified security messages to both drivers' and passengers' lives. To address these challenges, identity authentication systems have been introduced to the IoV to differentiate malicious vehicles and ensure traffic security.

In contrast to classic authentication systems, IoV authentication systems should provide basic functionality while also meeting the requirements of low delay, privacy protection, and high reliability. Moreover, the authentication burden on vehicles should be minimized. To preserve authentication privacy, traditional schemes have incorporated group signatures [2] and anonymity certificates [3] into existing IoV authentication systems. Furthermore, physically unclonable functions have been integrated into IoV authentication systems to enhance efficiency [4]. However, these schemes cannot ensure high reliability for IoV authentication systems, particularly in terms of resistance to single points of failure.

Currently, blockchain-based IoV authentication schemes have emerged as one of the most promising solutions for meeting the above reliability requirements [5]. With advanced features such as distributed architecture and tamper-proofing, applying blockchain to IoV authentication systems can enhance reliability, thus ensuring traffic security. Nevertheless, due to limitations in blockchain throughput, the initial schemes cannot meet the low-delay requirement in the IoV. Additionally, the transparency of blockchain technology poses a threat to vehicle privacy.

To overcome these drawbacks, several authentication schemes have explored the use of numerous optimization strategies. In terms of authentication delay, Shen et al. proposed integrating an off-chain batch processing model to reduce authentication delay. Meanwhile, the off-chain design also decreases the on-chain costs, consequently reducing the transaction fees paid to blockchain miners [6]. In terms of privacy, Zhang et al. introduced self-certified public key cryptography to protect authentication privacy [7]. Additionally, the scheme also enables vehicles to outsource most of the storage burden, which further improves the authentication efficiency. However, the scheme fails to provide resistance against de-anonymization attacks such as heuristic clustering attacks, thus compromising authentication privacy.

To resist de-anonymization attacks, several schemes have adopted novel privacy-preserving methods for authentication systems. Conditional privacy [8], [9], multi-signatures [10], and chameleon hash functions [11] have been integrated into blockchain-based IoV authentication systems. Nevertheless, to perform authentication, these schemes require vehicles

This work was supported by the Natural Science Foundation of China (NSFC) under Grants 62072426, U19B2023 and 61871362, and the Key Research and Development Program of Anhui under Grant 202104b11020029.

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

to store the whole blockchain, effectively running as full blockchain nodes, thereby imposing a heavy storage burden on vehicles. Moreover, these schemes also compromise the delay. In general, existing schemes fail to simultaneously meet all the requirements of IoV authentication systems.

In this paper, we introduce a light blockchain-based authentication scheme designed to fulfill all the requirements of the IoV. In terms of storage burden and privacy, our scheme introduces dynamic accumulators [12], allowing vehicles to outsource most of the storage burden to roadside units while maintaining the anonymous authentication of vehicles. Instead of the entire blockchain, a vehicle only synchronizes and verifies a subset of the blockchain, specifically, block headers, which contain accumulators, and its own pseudonym identities. These are significantly smaller in size—approximately 1,000 times smaller than the entire blockchain. Additionally, the customized strategy requires that each pseudonym identity is regularly replaced, providing resistance against heuristic clustering attacks.

In terms of reducing delay, we adopt an offline/online model, shifting the generation of identity proofs to an offline preprocessing phase to decrease delay in the online authentication phase. Furthermore, by dividing vehicles into multiple domains, we restrict the total number of vehicles added to each accumulator, thereby enhancing the preprocessing efficiency of dynamic accumulators. Finally, security analysis and experimental results demonstrate that the proposed scheme allows vehicles to perform mutual authentication efficiently without compromising privacy.

The remainder of this paper is organized as follows. Section II provides an overview of our system model, some assumptions and design goals. Section III presents the details of our scheme. A security analysis of the scheme is shown in Section IV. Section V evaluates the performance, and we conclude in Section VI.

II. PROBLEM STATEMENT

A. System Model

As shown in Fig. 1, our scheme involves three entities: Registration Authorities (RAs), Roadside Units (RSUs), and vehicles.

RAs: RAs offer authentication and registration services for vehicles and RSUs within the Internet of Vehicles, operating under the authority of government traffic management departments. To support this, RAs maintain full blockchain nodes, enabling them to synchronize and verify all transactions. Additionally, they can organize registered vehicles into multiple domains, significantly reducing authentication delays between vehicles.

RSUs: RSUs, running full nodes, assist vehicles in conducting authentication efficiently. Compared to connecting directly to RAs, connecting to RSUs can enhance the efficiency of synchronizing block headers and generating proofs.

Vehicles: vehicles run as light nodes in the IoV authentication system. Once registered, vehicles can utilize the private key of the key pair to update their pseudonym identity set, and they can also authenticate other vehicles' pseudonym identities within the IoV system. After synchronizing block headers and generating proofs, vehicles can engage in two-way authentication without connecting to RSUs, thereby reducing delays.

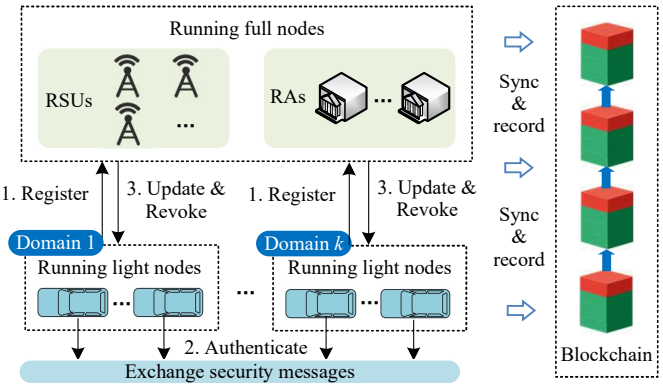


Fig. 1: **System model**

B. Threat Model

We assume that the RAs and RSUs are normally trustworthy in IoV authentication systems. However, RSUs may crash due to failures or external attacks, posing a threat to the security of the authentication system. Moreover, malicious attackers may utilize fake identities to access the IoV system and disseminate falsified security messages, such as fake maps, thereby endangering the driving security of honest vehicles. Furthermore, they can also register as a vehicle to gain access to the system. Additionally, attackers can gain access to public blockchains or pose as honest vehicles to gather security messages, such as vehicle driving traces and certificates, enabling them to infer real identities. Moreover, they can also employ a heuristic clustering attack to further enhance the accuracy of inference.

C. Design Goals

Security: Attackers using fake identities are effectively prevented from accessing the authentication system. Even if attackers successfully register as vehicles, the proposed scheme enables RAs to revoke their registrations upon detecting the transmission of falsified security messages. Furthermore, even in scenarios where RSUs are compromised by attackers, the proposed scheme ensures that vehicles can still perform authentication securely.

Privacy: The proposed scheme should enable vehicles to conduct authentication in a privacy-preserving manner. Even if attackers register as vehicles and employ a heuristic clustering attack, they cannot accurately infer the real-world identity of vehicles.

Efficiency: Without synchronizing the entire blockchain, the proposed scheme should minimize the authentication delay of vehicles to meet the requirement.

III. SYSTEM DESIGN

A. System Initialization

Before providing authentication services, RAs and RSUs need to deploy smart contracts and register their identities.

Each RA utilizes the Elliptic Curve Digital Signature Algorithm (ECDSA) to generate a pair of keys (a public key pk and a private key sk) and their corresponding addresses. Subsequently, they deploy smart contracts while uploading these public keys. Following this, RSUs generate their key pairs and addresses and register their public keys with smart contracts. When connecting to RSUs, vehicles can use these public keys to verify the RSUs.

After registration, RAs need to generate and upload accumulators to smart contracts to complete system initialization. Specifically, RAs call Algorithm 1 to generate an accumulator. RAs select two large prime numbers p and q and calculate the security parameter $N = pq$ as in the RSA accumulator system. Note that only N should be uploaded to the smart contracts, while p and q are discarded. Subsequently, based on the pre-set number of domains k, RAs select k random values $g_i \in \mathbb{Z}_N^*$, where $1 \leq i \leq k$, to generate the accumulator set S, completing the initialization.

Algorithm 1: Accumulator Initialization

Input: k
Output: S
$p, q =$ SelectLargePrimes()
$N = p \cdot q$
$S = \varnothing$
for $i \leftarrow 1$ **to** k **do**
  $g_i =$ SelectRandomValueIn$(\mathbb{Z}_N^*)$
  $s_i = g_i$
  $S = S \cup s_i$
end

B. Vehicle Identity Registration

Before authenticating and exchanging security messages, vehicles should first register their identities within the IoV through RAs. Initially, a vehicle sends a registration request to an RA, containing its real-world identity *RID*, such as the license plate number, and a list of public keys $\{pk_1, \cdots, pk_n\}$. Upon receiving the request, the RA verifies the validity of the real identity. Otherwise, the RA rejects the request. Otherwise, the RA selects a domain and utilizes its accumulator s_j, where $1 \leq j \leq k$, to register the vehicle's identity. Note that our scheme limits the total number of vehicles in a domain to ensure the efficiency of the vehicle identity revocation and update process. The parameters are set by RAs. If all domains are at full capacity, RAs generate a new accumulator and upload it to the smart contracts.

In addition to selecting a domain, the RA also sets pk_1 as the vehicle update public key and uploads it to the smart contracts through a registration transaction. Then, the vehicle can use the corresponding private key sk_1 to upload its pseudonym identity set to the smart contracts, completing the vehicle identity registration. Furthermore, the RA also stores the set $\{pk_2, \cdots, pk_n\}$ as the vehicle's pseudonym identity set for the revocation process in Section III-D.

After the updated public key is included in the smart contracts, the vehicle conducts offline preprocessing to complete the identity registration. As shown in Algorithm 2, the vehicle generates witnesses for each pseudonym identity's public key. For instance, the witness of pk_2, denoted as w_2, is calculated as $(s_i)^{t_2}$, where s_i is the accumulator and $t_2 = \prod_{j=3}^{n} pk_j \ \textit{Mod}\ N$, and the witness of pk_3, denoted as w_3, is calculated as $(s_i)^{t_3}$, where $t_3 = \prod_{j=2, j\neq 3}^{n} pk_j \ \textit{Mod}\ N$. After completing the witness generation, the vehicle updates the accumulator and submits the result $s_i = (s_i)^{pk_{prod}}$, where $pk_{prod} = \prod_{j=2}^{n} pk_j \ \textit{Mod}\ N$, to the RA through a transaction. Upon receiving the transaction, the RA verifies the result s_i according to the pseudonym identity set it has stored. If the verification is successful, the transaction is submitted to the blockchain to finalize the identity registration.

Algorithm 2: Offline Preprocessing of Vehicles

Input: $s_i, \{pk_2, \cdots, pk_n\}$
Output: pk_{prod}, s_i, W
$W = \varnothing$
for $k \leftarrow 2$ **to** n **do**
  $t_k = \prod_{j=2, j\neq k}^{n} pk_j \ \textit{Mod}\ N$
  $w_k = (s_i)^{t_k} \textit{Mod}\ N$
  $W = W \cup w_k$
end
$pk_{prod} = \prod_{j=2}^{n} pk_j \ \textit{Mod}\ N$
$s_i = (s_i)^{pk_{prod}} \textit{Mod}\ N$

C. Authentication of Vehicle Identity

After registering their identities, vehicles can participate in the IoV and exchange security messages. Note that vehicles should conduct identity authentication before engaging in any exchange. To conduct authentication, the vehicle should synchronize and verify the blockchain headers while registering its identities. When a new block is generated, the vehicle can synchronize and verify blockchain headers through RSUs. Before exchanging security messages, the vehicle authenticates another vehicle through the accumulators in the block headers. For clarity, we demonstrate the process of another vehicle (known as a target vehicle) authenticating the vehicle. Naturally, this vehicle can authenticate a target vehicle through the same process.

To conduct the authentication, the vehicle should select a pseudonym identity (assuming it is pk_i, where $1 \leq i \leq k$ and it has been added to the accumulator s_u) and send it along with the witness data to the target vehicle. After receiving the identity and the witness data, including pk_i, w_i, and the domain number of the accumulator s_u, the target vehicle conducts the authentication.

Initially, the target vehicle utilizes the domain number u to obtain the accumulator s_u from the most recent block header it has stored. Then, the target vehicle verifies equation $(w_t)^{pk_i} ?= s_u$. If successful, it indicates that the vehicle is a registration vehicle. After completing two-way authentication, vehicles can proceed to exchange security messages. Note that to resist heuristic clustering attacks, we have implemented a customized strategy, where each pseudonym identity can only

be used for a certain period of time, such as one day. The vehicle then replaces it with other unused pseudonym identities in the pseudonym identity set.

D. Vehicle Identity Revocation & Update

In our scheme, if a registered vehicle sends incorrect security messages to other vehicles, the RAs should revoke their identities. Additionally, since our scheme applies the customized pseudonym identity strategy, vehicles need to update their pseudonym identities when the identities are exhausted. Since pseudonym identities must be revoked during the update process, let us first delve into the details of revoking a registration identity.

Upon receiving evidence of a registered vehicle engaging in malicious behavior, the RA revokes the vehicle's identity. When a vehicle receives incorrect security messages, it uploads these messages as evidence to an RA along with the pseudonym identity of the malicious vehicle. Through the stored pseudonym identities, RAs can accurately distinguish all identities of the malicious vehicle. Subsequently, the RA calls Algorithm 3 to revoke the identities of the malicious vehicle. For convenience, we assume that the identities of the malicious vehicle are registered in domain (accumulator) s_u and that its update public key is pk_m. Moreover, the vehicles' pseudonym identity sets in the accumulator are $pk_{prod1}, \cdots, pk_{prodd}$, and the set of malicious vehicles is pk_{prodm}. In Algorithm 3, the RA should reconstruct a new accumulator s_u and then adds the pseudonym identity sets of the other honest vehicles in the domain to s_u.

Algorithm 3: Vehicle Identity Revocation

Input: $\{pk_{prod1}, \cdots, pk_{prodd}\}$
Output: s_u

$s_u = \text{SelectRandomValueIn}(\mathbb{Z}_N^*)$
for $i \leftarrow 1$ **to** d **do**
  if $i \neq m$ **then**
    $s_u = (s_u)^{pk_{prodi}} Mod\ N$
end

Once these sets have been added to s_u, the RA updates the accumulator set S. Specifically, the RA constructs a revocation transaction that contains s_u and publishes it to the blockchain to complete the revocation. Once the revocation transaction is included in the blockchain, the smart contracts replace the s_u in the block header. Furthermore, the revocation transaction also revokes the update keys of the malicious vehicle. Note that upon receiving the update, other vehicles should synchronize and update their pre-processed witnesses to avoid false positives in authentication.

During the identity update process, Algorithm 3 is also executed. The vehicle utilizes Algorithm 3 to delete all previously used pseudonym identities. Then, the vehicle generates a new pseudonym identity set and adds the set to the new accumulator. Subsequently, the vehicle signs and publishes an update transaction to the blockchain using its update private key. Before publishing the update transaction to the blockchain, the vehicle uploads the pseudonym identity set to an RA. The update transaction can be included in the blockchain once the RA verifies that the set matches the accumulator update. Once the transaction is on-chain, the smart contracts update the s_u, and other vehicles should also synchronize and update their preprocessed witnesses to prevent false positives in authentication. In contrast to the revocation transaction, the update transaction does not revoke the update key.

IV. SECURITY ANALYSIS

A. Security

The proposed scheme can meet the security requirement of the IoV authentication system. Initially, without registering as vehicles, attackers are unable to connect to honest vehicles through fake identities. Specifically, before establishing connections, vehicles conduct authentication with the counterparty through block headers and dynamic accumulator proofs. Without registering as vehicles, attackers cannot forge a registration transaction to add their fake identities to the dynamic accumulator, even in the event of RSU failures. As a result, they are unable to generate valid proofs and fail to authenticate and connect with legitimate vehicles. Consequently, attackers are unable to compromise traffic safety using fake identities.

Even if attackers register as vehicles, they still cannot endanger traffic security. Specifically, attackers can be identified if they transmit falsified security messages. Then these messages will be submitted as evidences to RAs. When receiving the submission, RAs immediately publish a revocation transaction to the blockchain to revoke the identity, and they also blacklist the real identities of the attackers. Consequently, attackers cannot utilize the real identities listed on the blacklist to register vehicle identities.

B. Privacy

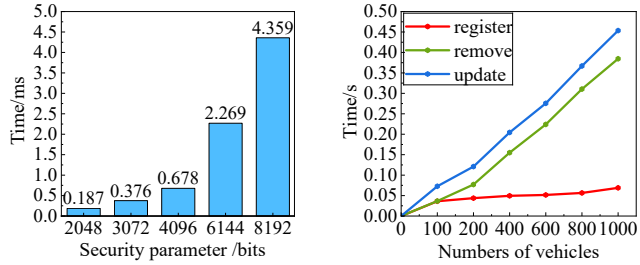
The proposed scheme emphasizes the privacy of vehicles. Initially, it allows vehicles to utilize pseudonym identities instead of real identities, thereby enhancing privacy. Even though attackers can access the public blockchain, they are unable to distinguish the real identities of vehicles. To compromise vehicle privacy, attackers may register as vehicles collect security messages, such as traces of other vehicles, and combine them with heuristic clustering attacks to distinguish their real identities. Fortunately, dynamic accumulators enable vehicles to conduct authentication without revealing pseudonym identities, thus preserving privacy. The customized pseudonym identity strategy can break the links between the different pseudonym identities of a single vehicle, thereby providing resistance against heuristic clustering attacks.

V. PERFORMANCE EVALUATION

In this section, we evaluate the performance the proposed IoV authentication scheme. We employ established implementations of the extensively adopted Hyperledger blockchain [13] and pyca/cryptography [14] to craft a prototype for evaluating performance. Each node, running in RAs, RSUs, and vehicles,

is equipped with an Intel Core i7-6700U processor and 8 GB of RAM. The network bandwidth between nodes is 1Gbps.

In summary, the performance of our scheme comprises two aspects: (i) the authentication delay and (ii) the delays associated with other processes, such as registration, preprocessing, update, and revocation. We begin by showing the performance of the authentication delay. As illustrated in Figure 2(a), we explore varying lengths of the RSA security parameter to assess the delay of the authentication phase. Across the common range of RSA security parameter lengths, from 2048 to 8192 bits, the authentication process of our proposed scheme scales exponentially with the security parameter lengths. Notably, even with an RSA security parameter as long as 8192 bits, our scheme ensures that vehicle authentication is completed in approximately 4.5 ms, aligning with the objectives outlined in Section II-C.



(a)Authentication delay (b)Other processes delays

Fig. 2: **Performance of our scheme**

Furthermore, we also evaluate the delay of other processes using the RSA security parameter with a length of 8192 bits and a domain encompassing a total vehicle count of less than 1000. As shown in Figure 2(b), the delay for each process scales linearly with the growth of the number of vehicles. Even in domains containing 1,000 vehicles, where each vehicle has 10 pseudonym identities, the delay of each process can be managed to approximately 0.5 seconds. It is worth noting that, except for the preprocessing process, all other processes require uploading a transaction to the blockchain, which takes approximately 2 seconds. This does not compromise the performance, as existing blockchain-based schemes also incur similar time requirements.

Finally, we compare our scheme with existing blockchain-based IoV authentication schemes across various aspects. As illustrated in Table I, unlike existing schemes, our scheme simultaneously meets all security, reliability, and privacy requirements while minimizing authentication delay. Additionally, our scheme introduces light nodes in vehicles, reducing the storage burden on vehicles.

VI. CONCLUSION

Currently, blockchains have been integrated to enhance the reliability of IoV authentication systems. However, existing blockchain-based schemes fail to maintain anonymity while minimizing both vehicle storage overhead and authentication delay. To address these challenges, we initially incorporate a dynamic accumulator and a pseudonymous identity update strategy to reduce the storage burden on vehicles while preserving anonymous vehicle authentication. Furthermore, we adopt an offline/online model and a multi-domain strategy to reduce delay and enhance efficiency. In general, our scheme offers superior efficiency, security, and privacy guarantees in contrast to existing schemes.

TABLE I: The comparison of our scheme to existing schemes

Scheme	Authentication delay	Security & Reliability	Vehicles storage	Privacy
Zhang's scheme [7]	0.650 ms	✓	✗	✗
Sutrala's scheme [8]	1.772 ms	✓	✗	✓
Cheng's scheme [9]	1.330 ms	✓	✗	✓
Xie's scheme [11]	0.200 ms	✓	✗	✓
Our scheme	0.187 ms	✓	✓	✓

REFERENCES

[1] B. Hildebrand, M. Baza, T. Salman, S. Tabassum, B. Konatham, F. Amsaad, and A. Razaque, "A comprehensive review on blockchains for internet of vehicles: Challenges and directions," *Computer Science Review*, vol. 48, pp. 100 547–100 574, February 2023.

[2] M. Cui, D. Han, and J. Wang, "An efficient and safe road condition monitoring authentication scheme based on fog computing," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9076–9084, July 2019.

[3] M. Azees, P. Vijayakumar, and L. J. Deboarh, "Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, February 2017.

[4] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, "A lightweight authentication and attestation scheme for in-transit vehicles in iov scenario," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14 188–14 197, November 2020.

[5] X. Wang, H. Zhu, Z. Ning, L. Guo, and Y. Zhang, "Blockchain intelligence for internet of vehicles: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2325–2355, August 2023.

[6] M. Shen, H. Lu, F. Wang, H. Liu, and L. Zhu, "Secure and efficient blockchain-assisted authentication for edge-integrated internet-of-vehicles," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 12 250–12 263, July 2022.

[7] X. Zhang, H. Zhong, J. Cui, I. Bolodurina, and L. Liu, "Lbvp: a lightweight batch verification protocol for fog-based vehicular networks using self-certified public key cryptography," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5519–5533, March 2022.

[8] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5535–5548, March 2020.

[9] G. Cheng, J. Huang, Y. Wang, J. Zhao, L. Kong, S. Deng, and X. Yan, "Conditional privacy-preserving multi-domain authentication and pseudonym management for 6G-enabled IoV," *IEEE Transactions on Information Forensics and Security (Early Access)*, September 2023.

[10] V. Srivastava, S. K. Debnath, B. Bera, A. K. Das, Y. Park, and P. Lorenz, "Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for internet of vehicles environment," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 9853–9867, May 2022.

[11] X. Xie, B. Wu, and B. Hou, "Bephap: A blockchain-based efficient privacy-preserving handover authentication protocol with key agreement for internet of vehicles," *Journal of Systems Architecture*, vol. 138, pp. 102 869–102 882, March 2023.

[12] D. Boneh, B. Bünz, and B. Fisch, "Batching techniques for accumulators with applications to iops and stateless blockchains," in *Annual International Cryptology Conference*, Santa Barbara, USA, 2019.

[13] "Hyperledger fabric," Github. [Online]. Available: https://github.com/hyperledger/fabric

[14] "Welcome to pyca/cryptography," Github. [Online]. Available: https://github.com/pyca/cryptography/blob/main/docs/index.rst